Workshop on Biometrics and e-Authentication

Security Issues, Threats and Countermeasures

Philip Statham - CESG Biometrics Programme Manager

philip.statham@cesg.gsi.gov.uk

Overview

- Overview of biometric security issues
- Technical threats and countermeasures
- Practical Investigations by CESG
- Conclusions

Security Threats – Broad Issues

- ***Threats against the System***
- ***Threats against the User***

Security Issues

- User security issues
- Application security issues
- Technical security issues
- Legal issues

- Boundaries are often fuzzy

User Security Issues

- Take biometric without consent
- Use of biometric identification by stalker
- Reliance on single strong id fails badly
- Database search for criminal suspects
- Administrator knows who matches me
- Function creep
- Biometric / audit trail reveals personal information
- System not as secure as we are told

Application Security Issues

- Application dependent
- Legal, human, financial
- Confidentiality, integrity, availability
  - Biometrics do not provide absolute identification
  - Biometrics are not secret
  - Biometrics are not random enough
  - Biometric algorithms are proprietary and not validated
  - Biometrics cannot be changed when compromised
  - Biometrics should only be stored on smart-cards
  - Biometrics do not offer non-repudiation

Technical Security Issues

- Technology dependent
- Application neutral
  - Performance limitations
  - Enrolment quality and integrity
  - Spoofing (physiological biometrics)
  - Mimicry (behavioural biometrics)
  - Latent/Residual Images
  - Template integrity/confidentiality
  - Capture/replay attacks

Technology Solutions

- Liveness checks
- Template encryption/signing
- Binding template to application
- Locking template to user consent
- Cancellable biometrics
- Data communication encryption
- No central database
- Duress codes
- Transaction log & audit trail

Procedural Security Solutions

- Trustworthy staff
- Security training for staff
- Separation of roles
- Supervised operation
- Security audit
- User audit
- Legal compliance
- Codes of conduct

e-Authentication Security Threats

- Service Point Threats
  - Unauthorised person gaining access
  - Verification – validity check against claimed id (1:1)
  - Security depends on ***False Accept Rate***
  - N.B. Maybe background check against watch list (1:n)?

- Registration Threats
  - Multiple IDs
  - Check against database for multiple enrolments (1:n)
  - Security depends on ***False Reject Rate***

Possible User Intentions

- To be identified/verified as themselves – the normal case
- To impersonate another enrolled user
  - Impostor copies other user's biometric (with or without collusion)
  - Both users employ same (bogus) biometric (implies collusion)
- To fail to be recognised as being already enrolled

Security is a Holistic Concept

- Technology can't solve all the problems
- All technology is imperfect
- Real security comes from a mutually supportive combination of:

Some Biometric Security Technical Considerations

- Image quality checks
- Liveness checking
- Signal capture/replay
- Biometric Data Protection

Image Acquisition Quality Control

- How realistic do the presented biometric features need to be?
- What will the device accept for enrolment and normal use? e.g.
  - Null image?
  - “Trivial” images?
  - Noisy images?

Liveness Checking

- Detection of signs of liveness
- Detection of known artefacts
- Simultaneity
  - Same time and place as image acquisition occurs
  - Not always realised in practice
- May be provided by hardware and/or software
  - Software has advantage of inherent simultaneity
- It's a hard problem!

Signs of Liveness

- Intrinsic Properties
  - **Physical**: Weight, density, elasticity
  - **Electrical**: capacitance, resistance, impedance
  - **Visual**: colour, opacity, appearance, shape
  - **Spectral**: transmittance, reflectance, absorbance
  - **Body fluid**: oxygen, blood constituents, DNA
- Involuntary signals
  - Pulse
  - Blood pressure
  - Blood flow
  - Heat & Thermal gradients
  - Transpiration
  - Perspiration
  - ECG – electrical signals generated by the heart
  - EEG – brain wave signals
- Voluntary/involuntary response to a stimulus: challenge-response

Signs of Artefacts – e.g.

- Silicone/gelatin finger
- Photograph
- Contact lens
- Mask
- Tape recording

Signal Capture/Replay

Are the signals protected?

- Physical protection
  - Self contained unit
  - Tamper proof
  - armoured cable
- Logical protection
  - encryption
  - time stamping
  - challenge - response

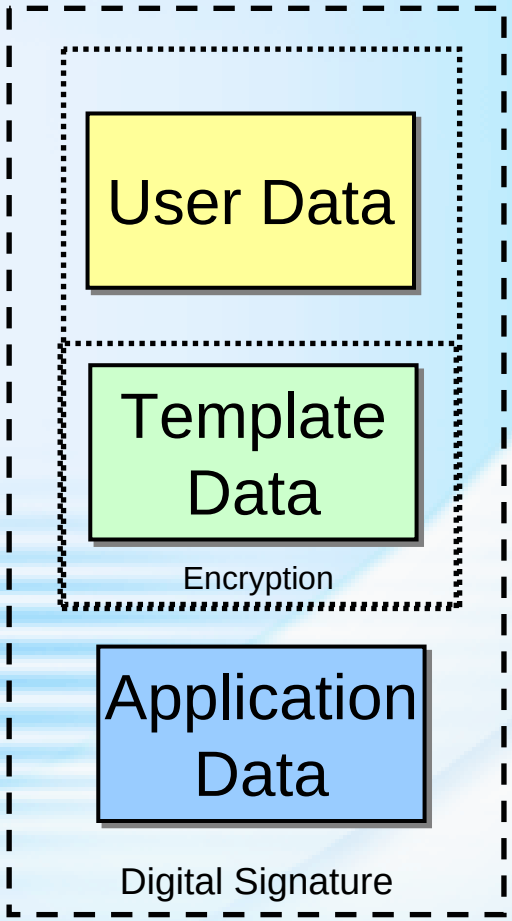
Can the signals be reconstructed easily?

Template Integrity

- Template database or stored on card?
- Access control to template database
- Tamper resistance of smartcard
- Can the system detect if someone has added or changed a template?
  - Template signing – integrity
  - Template encryption – confidentiality (and integrity)

Protecting the Biometric Data

- Issues
  - **Integrity** – Protection against removal, replacement or alteration - digital signing
  - **Confidentiality** – Protection against unauthorised disclosure - encryption
- Bind the data to the application



For further information see:
www.bioscrypt.com/assets/Biometric_System_Security.pdf

Published Ad-hoc "Evaluations"

- Six biometric devices point their finger at security
  - Network computing – Jun 1998
    - Fingerprint
- Biometrics security
  - PC magazine – Feb 1999
    - Fingerprint / face / voice
- Fingerprint recognition–don't get your fingers burned
  - Van der Putte, Keuning, Jan 2000
- Impact of artificial "gummy" fingers
  - Matsumoto, Jan 2002
- Biometric access devices & programs put to the test
  - c't magazine, may 2002
  - Fingerprint / face / iris

Biometric Security Assessment Programme

- Develop methodology to support security evaluations
- Practical investigation programme
  - Develop CESG knowledge
  - Validate and refine methodology
  - Informal appraisal of product security
  - Feedback findings to companies to promote future security improvements

Investigation Areas

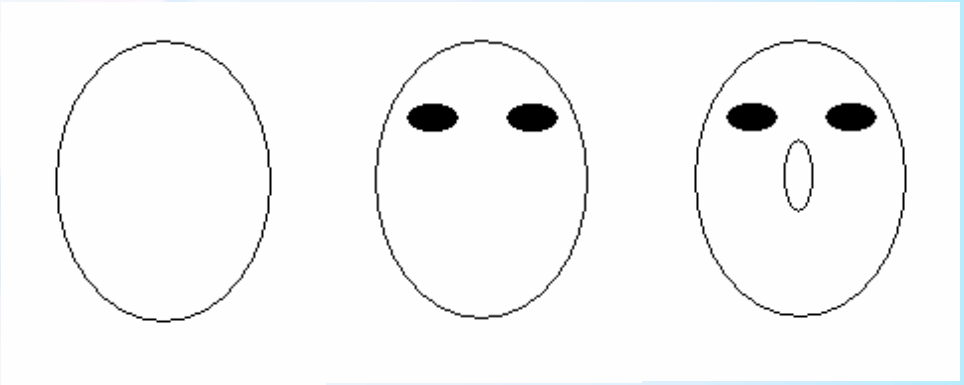
- Casual Impostor/Zero Effort Attacks
- Easy/Weak Template Generation
- Access to Template/Data Store
- Spoofing – Artificial Attempts, Mimicry and Fakes
- Wire Snooping and Replay

- Face
- Fingerprint
- Iris

Face Recognition Tests

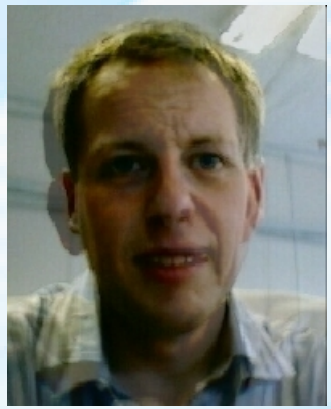
Image Acquisition Criteria

Enrolling Simple/Easy Images



Success:	No	No	Yes

Authenticating against enrolled user with photographs and morphed images

A	B	Paper print of A	(A&B Morphed)
			

Livecheck off - Yes

Livecheck on – Yes but with difficulty

Face Recognition Tests

Effect of Disguise

Enrolment / Reference Image

Normal ID: 0.767342

0.762008

0.76242

0.736215

0.707423

0.723648

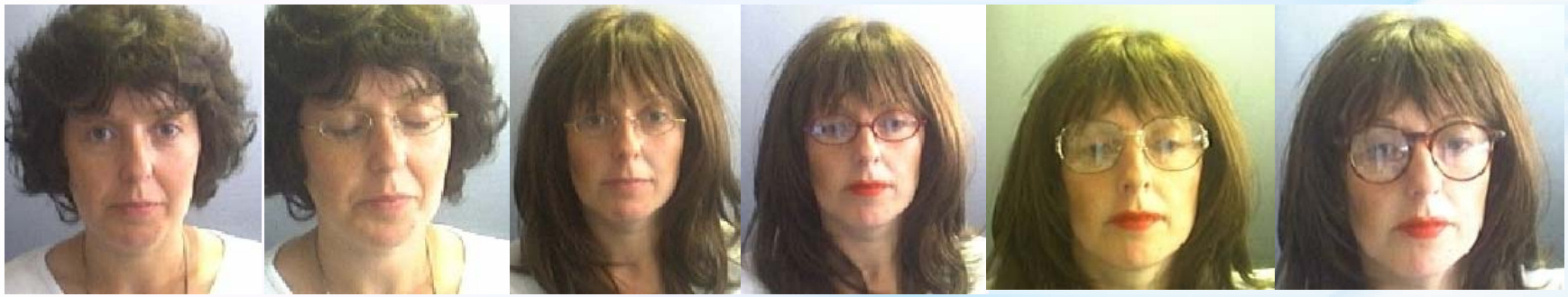
0.66777

Face Recognition Tests

Effect of Disguise

Enrolment / Reference Image

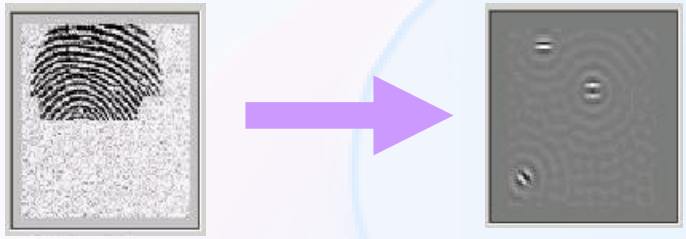
Normal ID: 0.788537



0.75622 0.713133 0.73317 0.72323 0.71426 0.716726

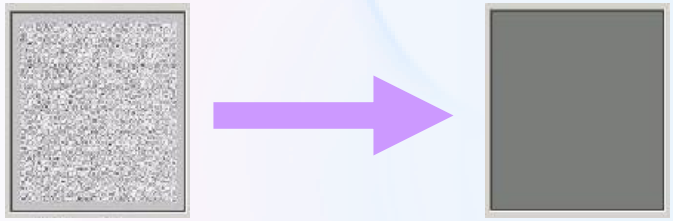
Fingerprint - Image Quality Control

Portion of finger on sensor



Template with few features

Lifting finger on/off sensor



Null image / template

Multiple fingers on sensor

Either finger can be used at authentication (two fingerprints on one template)

Non-fingerprint images

Drawing on a thin piece of tissue paper can be enrolled and used at authentication

Wire Snooping

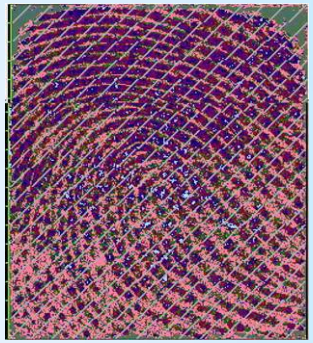
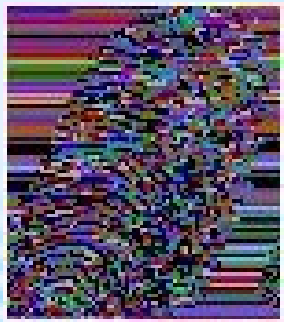
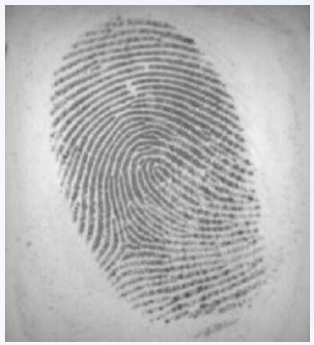
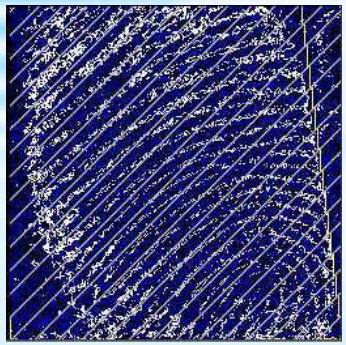
	Real	Reconstruction
CCD 1 (USB)		
CCD 2 (Ethernet)		
Optical (USB)		

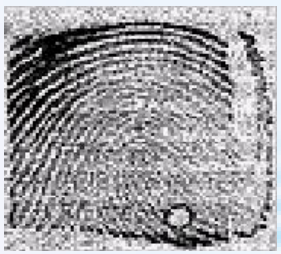
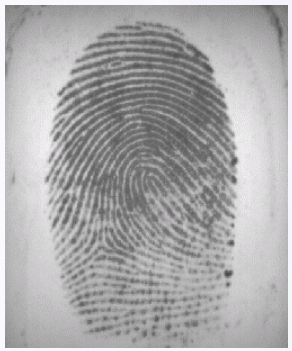
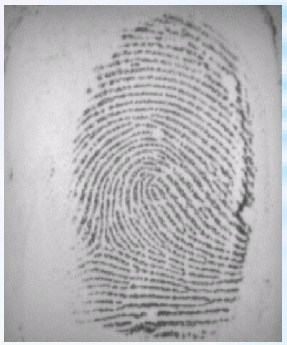
Image Reconstruction from Stored Images

Original

Reconstruction

Templates are often not encrypted

Spoof Fingertips

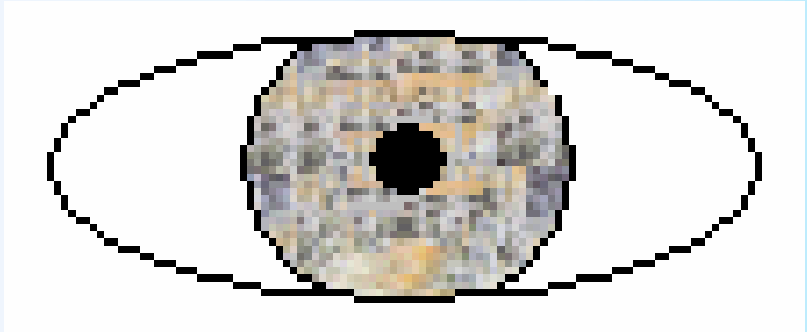
	Real	Spoof
CCD 1		
CCD 2		
Optical		

Successful enrolment and authentication with spoof fingertips

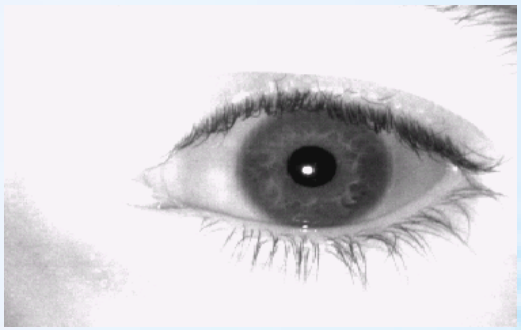
Note: This is a cooperative effort

Iris Recognition Tests

Constructing fake irises (used at enrolment and authentication)



Enrolling and authenticating with printed images of irises



Satisfy primitive liveness checks with:

- **Live eye behind pin hole in pupil**
- **Soft contact lens placed over iris**
- **White dot of correction fluid**

Enrolment/Quality Control – Sophisticated Camera

- Attempts at enrolling poor quality images unsuccessful – Camera appeared to implement good image quality control checks

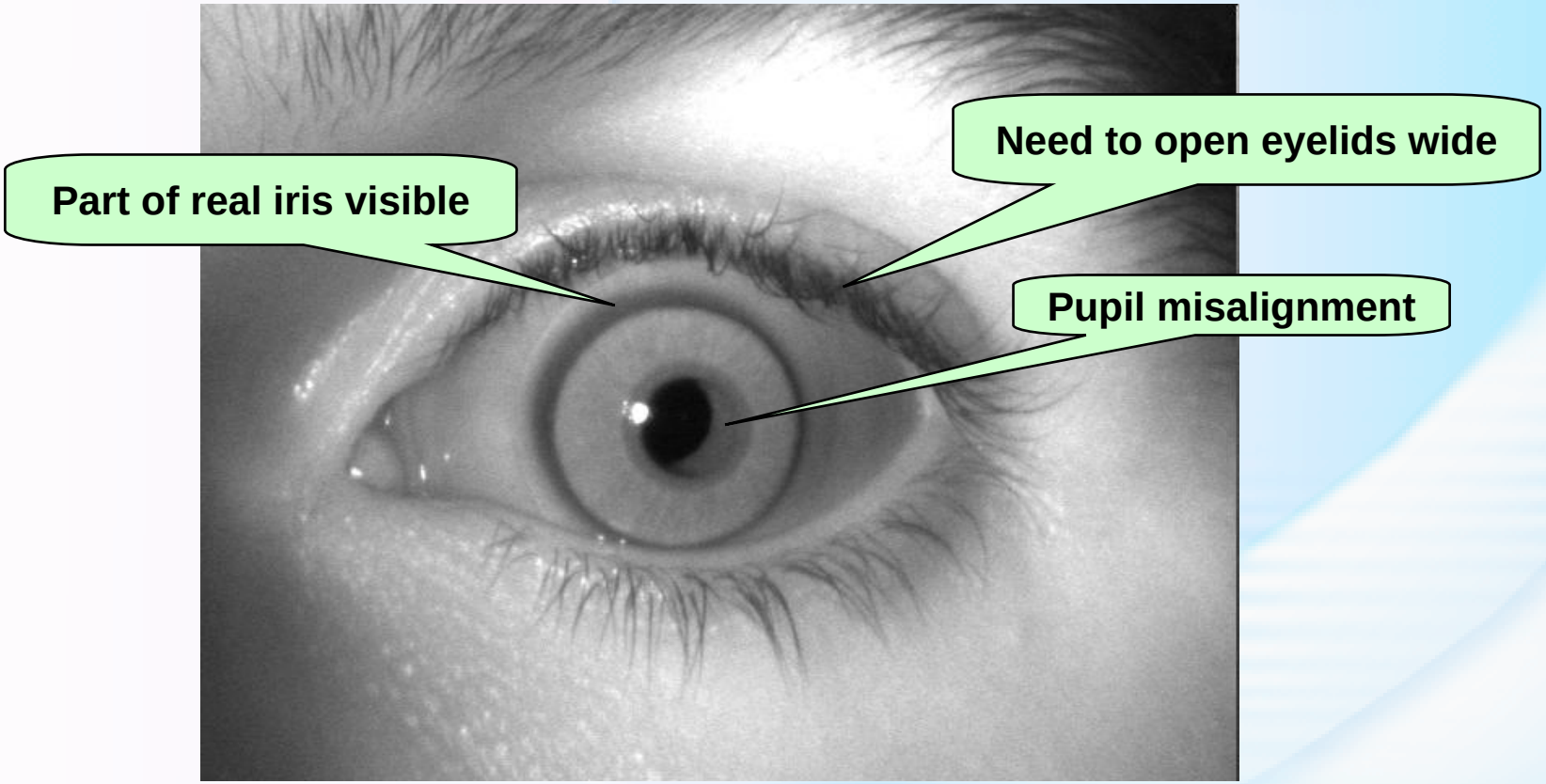
Not possible to enrol images like this

- System requires good portion of the iris to be visible both at enrolment and authentication

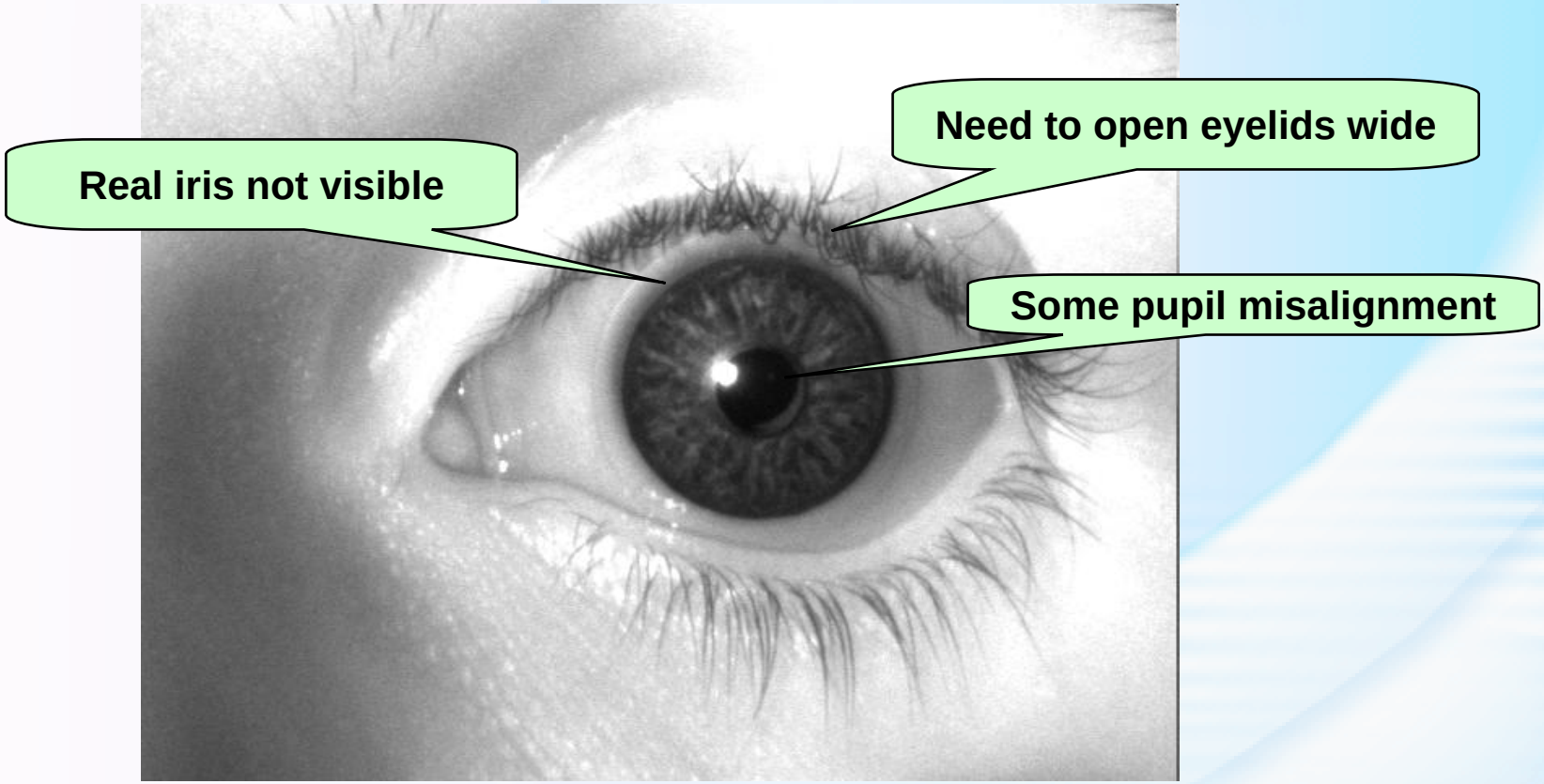
Experiments with Patterned Contact Lenses

- Normal patterned lenses are semi-transparent
  - Resulting enrolled iris pattern is part lens, part eye
- Opaque layered lenses are available from manufacturers
- What we got to begin with:
  - Blue hand-painted lens with stabilisation – grey opaque layer
  - Brown screen printed lens with stabilisation – black opaque layer
- What we tried:
  - Normal enrolment and verification using same eye
  - Attempt to re-enrol using same lens
  - Enrolment with one eye, verification using other eye
- Several cameras of different levels of sophistication

Brown Screen Printed Lens



Blue Hand Painted Lens



Patterned Contact Lens Tests

Enrolment sometimes possible with patterned lenses.

Underlines the importance of good liveness checks.

Summary of Results

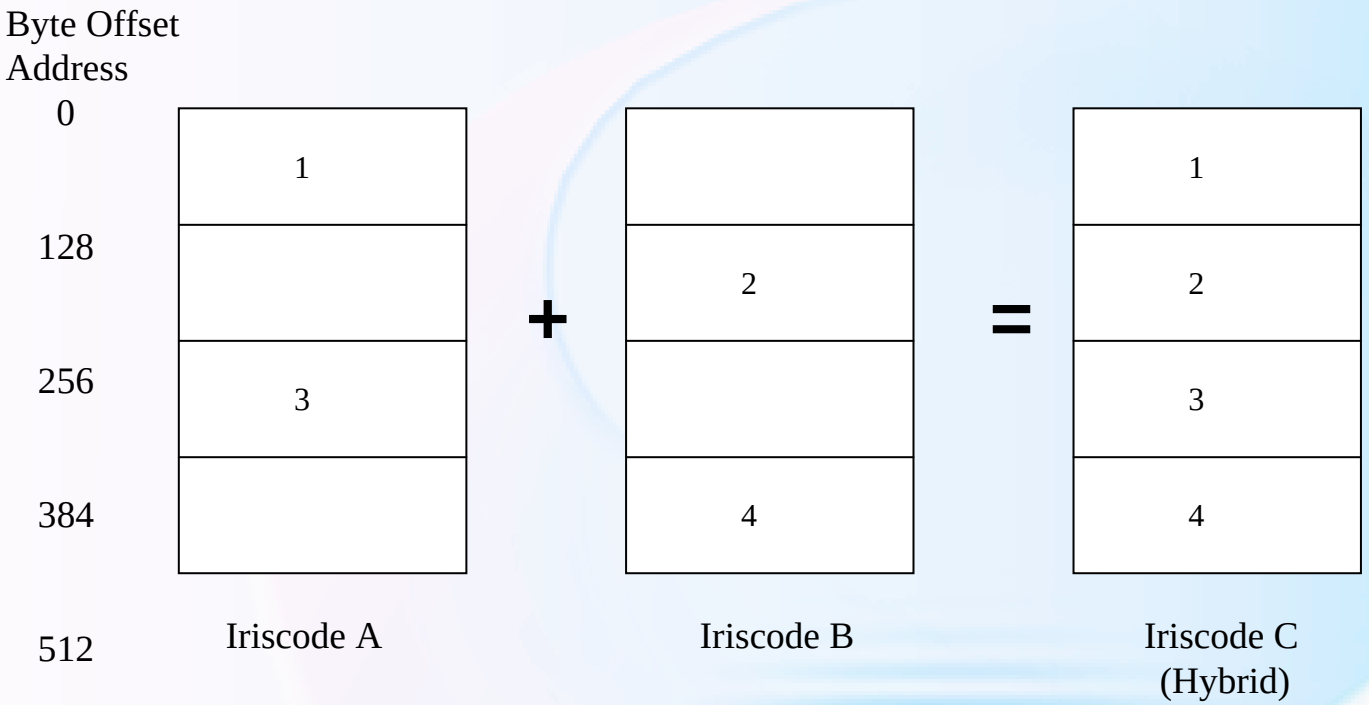
	Simple Camera				Sophisticated Camera			
	Enrolment	Verification	Multiple Enrolment	Different Eye	Enrolment	Verification	Multiple Enrolment	Different Eye
Brown Lens	Y	Y	N	Y	Y*	Y*	N	Y
Blue Lens	Y	Y	N	Y	N	N	-	-

* Sometimes, with difficulty

Access to Template/Data Store

- Backend database is implemented in Microsoft Access – Password Protected
- Password can be cracked with recovery software from the Internet
- Possible to remotely manipulate data within the database from a laptop connected to the same network as the server machine.
- Iriscodes can be extracted from tables within the database
- Possible to modify, delete and inject new identities into database, undetected by the system.

One Danger of Unprotected Database - Hybrid Iriscodes



Possible to place two identities within one iriscode e.g.

Take two distinct iriscodes from Persons A and B, extract two 128-byte chunks of iriscode data from each template, and replace in a new file, in their original bit positions. Write the new iriscode to the database as Person C.

Result: Person A and B can both match as Person C.

Conclusions for Iris Cameras

- Sophisticated cameras have good quality control checks
- Spoofing possible with simple cameras
- Spoofing sometimes possible but with difficulty on sophisticated cameras
- Backend database protection is often poor
  - Possible to modify delete and add new identities, undetected by the system
  - Possible to combine data from two iriscodes to create a hybrid iriscode

Future Work Needed to Address

- Performance improvements (FAR/FRR)
- Anti-spoofing technology
- Security assurance
  - More evaluations
  - Security assurance methodology
- Template binding
  - User – template – application – consent
- Specification of security for
  - Large-scale implementations
  - Interoperability
  - Integration with other security technology